What Is Claimed Is:

1. A multicast communication system having a multicast server for transmitting data relating to a prescribed data distribution service by multicasting, and a plurality of clients belonging to a multicast group and receiving said data,

said multicast server comprising:

a data encryption unit for encrypting said data by using a first encryption key;

a data transmission unit for transmitting said data encrypted by said data encryption unit to said plurality of clients by multicasting;

a key encryption unit for encrypting said first encryption key by using a second encryption key; and

a key transmission unit for transmitting said first encryption key encrypted by said key encryption unit by unicasting to at least one of the plurality of clients, said at least one client subscribing to said data distribution service; and

said at least one client comprising:

a key reception unit for receiving said encrypted first encryption key transmitted by said transmission unit;

a key decryption unit for decrypting said encrypted first encryption key received by said key reception unit, using a decryption key; and

a data decryption unit for decrypting the encrypted data transmitted by said data transmission unit, using the first encryption key obtained by said decryption unit.

2. The multicast communication system according to claim 1, wherein said multicast server further comprises a registration unit for registering a client of the plurality of clients, that wishes to subscribe to said data distribution service.

3. The multicast communication system according to claim 1, wherein said multicast server further comprises a charging unit for applying quantity-based charges to said at least one client in accordance with the time or quantity of data received.

4. The multicast communication system according to claim 2, wherein said multicast server further comprises:

a deletion data reception unit for receiving deletion data indicating that the client registered by said registration unit has been deleted at least said first encryption key held by said client itself, said deletion data being transmitted from said client; and

an erasure unit for erasing from said registration unit the client that has transmitted said

deletion data, when said deletion data reception unit receives said deletion data; and

wherein said client further comprises:

a deletion unit for deleting at least said first encryption key held by said client itself in the event of withdrawal from said data distribution service; and

a deletion data transmission unit for generating said deletion data and transmitting said deletion data to said multicast server.

5. The multicast communication system according to claim 1, wherein said second encryption key and said decryption key are the same key.

6. The multicast communication system according to claim 5, wherein both said second encryption key and said decryption key are separately provided in respective clients subscribed to said data distribution service.

7. The multicast communication system according to claim 5, wherein said decryption key is constituted of hardware circuitry or a semiconductor chip.

8. The multicast communication system according to claim 1, wherein said second encryption key is a key that is obtained by said at least one client encrypting said first decryption key using a public key of said multicast

server and transmitting said encrypted first decryption key to said multicast server, and said multicast server decrypting said encrypted first decryption key using its own secret key.

9. The multicast communication system according to claim 1, wherein said second encryption key is a public key of a digital certificate issued by the public key infrastructure in respect of a client that has subscribed to said data subscription service, and said decryption key is a secret key of said digital certificate.

10. A multicast communication method carried out between a multicast server for transmitting data relating to a prescribed data distribution service by multicasting, and a client subscribed to said data distribution service of a plurality of clients that receive said data and belong to the multicasting group, said multicast communication method comprising steps of:

encrypting a first encryption key used in encryption of said data by using a second encryption key in said multicast server;

transmitting said encrypted first encryption key by unicasting to at least one of said plurality of clients in said multicast server, said at least one client subscribing to said data distribution service;

decrypting said encrypted first encryption key by using a decryption key, on receiving the encrypted first encryption key transmitted by said unicasting in said at least one client;

encrypting said data using said first encryption key in said multicast server;

transmitting said encrypted data by multicasting to the plurality of clients in said multicast server; and

decrypting said encrypted data by using said first encryption key obtained by decryption of said decryption key on receipt of said encrypted data in said at least one client.

11. A multicast data transmission device comprising:

a data encryption unit for encrypting data relating to a prescribed data distribution service by using a first encryption key;

a data transmission unit for transmitting said data encrypted by said data encryption unit by multicasting to clients belonging to a prescribed multicast group by multicasting;

a key encryption unit for encrypting said first encryption key by using a second encryption key; and

a key transmission unit for transmitting the first encryption key encrypted by said key encryption unit by unicasting to at least one of the clients belonging to said

multicast group, said at least one client subscribing to said data distribution service.

12. A multicast data transmission method for transmitting data relating to a prescribed data distribution service to clients belonging to a prescribed multicast group by multicasting, comprising steps of:

encrypting a first encryption key used in encrypting said data, by using a second encryption key;

transmitting said encrypted first encryption key by unicasting to at least one of the clients belonging to said multicasting group, said at least one client subscribing to said data distribution service;

encrypting said data by using said first encryption key; and

transmitting said encrypted data to the clients belonging to said multicast group by multicasting.

13. A multicast data receiving device for receiving data relating to a prescribed data distribution service transmitted by multicasting, comprising:

a key decryption unit for decrypting a encrypted first encryption key obtained by subscribing to said data distribution service;

a data reception unit for receiving said data encrypted by using said first encryption; and

a data decryption unit for decrypting the encrypted data received by said data reception unit, by using the first encryption key obtained by decryption of said key decryption unit.

14. A multicast data receiving method for receiving data relating to a prescribed data distribution service, said data being transmitted by multicasting, comprising steps of:

decrypting an encrypted first encryption key obtained by subscribing to said data distribution service;

receiving said data encrypted by using said first encryption key; and

decrypting said received and encrypted data using the first encryption key obtained by said decryption.

15. A multicast communication system having a multicast server for transmitting data relating to a prescribed data distribution service by multicasting and a plurality of clients belonging to a multicast group and that receive said data,

said multicast server comprising:

a key updating unit for updating a data encryption key for encrypting said data, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing, said data encryption key that is valid after the updating timing being in a

relationship that is obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

an updating key holding unit for generating or holding in advance said updating key;

a data encryption unit for encrypting said data using a data encryption key that is valid currently;

a data transmission unit for transmitting said data encrypted by said data encryption unit to said plurality of clients by multicasting;

a key encryption unit for encrypting the updating key corresponding to the data encryption key that is valid after the updating timing, at intervals of said updating timing, using the data encryption key that is valid after the updating timing; and

an updating key transmission unit for transmitting the updating key encrypted by said key encryption unit to at least one of said plurality of clients by unicasting or multicasting at intervals of said updating timing, said at least one client subscribing to said data distribution service; and

said at least one client comprising:

a data reception unit for receiving the encrypted data transmitted by said data transmission unit;

a data decryption unit for decrypting said encrypted data received by said data reception unit, using

a data decryption key that is valid currently that is the same as said data encryption key that is valid currently;

an updating key reception unit for receiving the encrypted updating key transmitted by said updating key transmission unit;

an updating key decryption unit for decrypting the encrypted updating key received by said updating key reception unit, using said data decrypting key that is valid currently; and

a data decryption key updating unit for updating a data decryption key that is valid before said updating timing to a data decryption key that is valid after the updating timing, at intervals of the updating timing, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating time to said data decryption key that is valid before the updating timing, a data decryption key on subscribing to said data distribution service being given from outside.

16. A multicast communication method carried out between a multicast server for transmitting data relating to a prescribed data distribution service by multicasting and at least one of a plurality of clients for receiving said data and belonging to the multicasting group, said at

least one client subscribing to said data distribution service, comprising steps of:

encrypting said data by using a data encryption key that is currently valid in said multicast server;

transmitting said encrypted data to said plurality of clients by multicasting in said multicast server;

decrypting said encrypted data by using a currently valid data decryption key that is the same as said currently valid data encryption key on receiving the encrypted data transmitted from said multicasting server in said at least one client;

updating the data encryption key, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing in said multicast server, said data encryption key that is valid after the updating timing being in a relationship that is obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

encrypting said updating key corresponding to the data encryption key that is valid after the updating timing by using the data encryption key that is valid after the updating timing at intervals of said updating timing, and transmitting the encrypted updating key to said at least one client by unicasting or multicasting in said multicast server;

decrypting the encrypted updating key by using a currently valid data decryption key on receiving the encrypted updating key transmitted from said multicasting server in said at least one client; and

updating a data decryption key that is valid before the updating timing to a data decryption key that is valid after the updating timing at intervals of the updating timing in said at least one client, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating time to said data decryption key that is valid before the updating timing at said intervals, a data decryption key on subscribing to said data distribution service being given from outside.

17. A multicast data transmission device, comprising:

a key updating unit for updating a data encryption key for encrypting data relating to a prescribed data distribution service, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing, said data encryption key that is valid after the updating timing being in a relationship that is obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

an updating key holding unit for generating or holding in advance said updating key;

a data encryption unit for encrypting said data using a data encryption key that is valid currently;

a data transmission unit for transmitting said data encrypted by said data encryption unit to clients belonging to a prescribed multicast group by multicasting;

a key encryption unit for encrypting the updating key corresponding to the data encryption key that is valid after the updating timing, at intervals of said updating timing, using the data encryption key that is valid after the updating timing; and

an updating key transmission unit for transmitting the updating key encrypted by said key encryption unit to said at least one of clients by unicasting or multicasting at intervals of said updating timing.

18. A multicast data transmission method for transmitting data relating to a prescribed data distribution service to clients belonging to a prescribed multicast group by multicasting, comprising steps of:

encrypting said data by using a data encryption key that is valid currently;

transmitting the encrypted data to the clients by multicasting;

updating the data encryption key, at intervals of a prescribed updating timing, to a data encryption key that

is valid after the updating timing, said data encryption key that is valid after the updating timing being in a relationship that is obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

encrypting said updating key corresponding to the data encryption key that is valid after the updating timing by using the data encryption key that is valid after the updating timing at intervals of said updating timing; and

transmitting the encrypted updating key to at least one of said clients by unicasting or multicasting.

19. A multicast data receiving device for receiving data relating to a prescribed data distribution service, said data being transmitted by multicasting from a multicast server, comprising:

a data reception unit for receiving said data encrypted by a data encryption key that is currently valid, of data encryption keys that are updated at intervals of a prescribed updating timing;

a data decryption unit for decrypting said encrypted data received by said data reception unit, using a data decryption key that is currently valid, said data decryption key being the same as said data encryption key that is currently valid;

an updating key reception unit for receiving from said multicast server a result of encrypting an updating key by using said data encryption key that is currently valid, said updating key being employed for updating said data decryption key;

an updating key decryption unit for decrypting said result received by said updating key reception unit, using said data decrypting key that is currently valid; and

a data decryption key updating unit for updating, at intervals of a prescribed updating timing, a data decryption key that is valid before said updating timing to a data decryption key that is valid after the updating timing, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating time to said data decryption key that is valid before the updating timing, a data decryption key on subscribing to said data distribution service being given from outside.

20. A multicast data receiving method for receiving data relating to a prescribed data distribution service transmitted by multicasting from a multicast server, comprising steps of:

receiving said data encrypted by a data encryption key that is currently valid, of data encryption keys that are updated at intervals of a prescribed updating timing;

decrypting the encrypted data by using a decryption key that is currently valid, said decryption key being the same as said data encryption key that is currently valid;

receiving from said multicast server, a result of encrypting an updating key by using said data encryption key that is currently valid, said updating key being employed for updating said data decryption key;

decrypting said result by using said data decrypting key that is currently valid; and

updating a data decryption key that is valid before the updating timing to a data decryption key that is valid after the updating timing at intervals of the updating timing, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating timing to said data decryption key that is valid before the updating timing at said intervals, a data decryption key on subscribing to said data distribution service being given from outside.